Qwest
607 14th Street, NW, Suite 950
Washington, DC 20005
Phone 303-383-6651
Facsimile 303-896-1107

Kathryn Marie Krause
Associate General Counsel

February 29, 2008

FILED VIA ECFS

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to the Federal Communications Commission's *Report and Order*,[1] Qwest hereby files its Annual 47 C.F.R. § 64.2009(e) CPNI Certification.

Please contact me at the above-listed information if you have any questions.

/s/ Kathryn Marie Krause

cc: Best Copy and Printing, Inc. (fcc@bcpiweb.com)
Enforcement Bureau, Telecommunications Consumers Division
(two copies via courier)

---

[1] *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007). *Also see*, Public Notice, DA 08-171, rel. Jan 29, 2008.

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket No. 06-36

Annual Section 64.2009(e) CPNI Certification for 2007

Date filed: February 29, 2008

Name of company covered by this certification: Qwest (for the following carrier affiliates)

Form 499 Filer ID:
808440 Qwest Corporation
814711 Malheur Home Telephone Company
807684 E Paso County Telephone Company
808439 Qwest Wireless LLC
808882 Qwest Communications Corporation
822734 Qwest LD Corp.

Name of signatory: Alwin Roberts

Title of signatory: Senior Vice President – Mass Markets

I, Alwin Roberts, am an officer of Qwest Corporation (a local exchange carrier). Acting as an agent of that company, and on behalf of the other companies identified above, I certify that I have personal knowledge that the various companies have established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how the various companies' procedures ensure that they are in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

None of the Qwest companies identified above have taken action in the courts or before state or federal regulatory bodies against data brokers in the past year because none of them have had justification to do so.

The company received two customer complaints between December 8, 2007 and December 31, 2007 alleging unauthorized access and release of CPNI. Qwest investigated each complaint and determined that each lacked factual support. As a result, Qwest did not report either of these complaints to the website maintained by the Federal Bureau of Investigation and the United States Secret Service, pursuant to the Commission's rules. In the first instance, the customer alleged that his Qwest online account had been accessed by an unknown individual and his log in and password had been changed. Based on its investigation, Qwest determined that the customer had forgotten the information he needed to access the online account he had created in 2004. Over the entire life of that account, no one made changes to the email address or log in. In the other case, a customer alleged that a Qwest sales representative spoke with her boyfriend about her account and that she had not authorized him on the account. Repeated attempts to reach the customer went unanswered and Qwest's business records associated with contacts with the customer during the relevant time period indicated that the customer had never otherwise raised the issue of unauthorized account access.

Signed Alwin Roberts
[Electronic signature]

EXHIBIT 1 TO COMPLIANCE CERTIFICATE
Qwest Statement of Operating Procedures

Below, Qwest describes its operating procedures to ensure compliance with the Federal Communications Commission ("FCC") Customer Proprietary Network Information ("CPNI") rules set forth in 47 C.F.R., Subpart U:

1. Al Roberts, Sr. Vice President in Mass Markets, is Qwest's CPNI Certifying Officer. Qwest also takes advantage of the expertise and experience of a variety of its other (non-sales) organizational units and personnel in addressing privacy and CPNI issues. Qwest has a Chief Privacy Officer ("CPO"), within the Risk Management organization, whose duties include advice and counsel on a variety of privacy issues. Within that Risk Management organization there is also an Information Security and Technology group, and technical CPNI issues are vetted with it. Still within that organization, Qwest has a dedicated CPNI Compliance Manager with more than a decade of experience in addressing and counseling on the proper uses of CPNI. That Compliance Manager, along with other Qwest Risk Management employees, including the CPO and the Information Security and Technology group, is responsible for assisting Qwest business units on a host of issues, including product development, training, discipline and supervision of marketing campaigns. Finally, all of the Qwest employees referenced above interact with senior Qwest legal counsel on CPNI matters that require legal analysis or advice. That counsel has been involved in CPNI issue for over 25 years. Qwest is confident that this cooperative and collaborative cross-discipline approach to CPNI issues creates an atmosphere and structure to ensure compliance with the FCC's CPNI rules.

2. In order to ensure that CPNI issues are resolved uniformly across the business and in a timely manner, the CPNI Compliance Manager hosts bi-weekly (and if necessary weekly) CPNI conference calls which are attended by senior CPNI legal counsel. When appropriate, members of the business units, Qwest's CPO, or other Qwest attorneys will attend these calls. During these calls, CPNI issues are discussed, issues are raised, and solutions are reached and/or action plans are established. In addition, the CPNI Certifying Officer is consulted or advised as necessary.

3. In addition to the "management" structure associated with addressing CPNI issues, all Qwest employees receive general annual training on CPNI rules. Employees with direct sales, marketing and product responsibilities receive additional and more-detailed training on the proper use of CPNI. The training includes instruction on how to properly address CPNI issues during inbound sales calls, and instruction to sales personnel on how CPNI may and may not be used during outbound marketing campaigns. Qwest uses these materials in face-to-face training sessions, at times, and posts them on Qwest's internal web site for easy access and consultation. Further, on an ongoing basis, targeted, niche training is conducted as needed.

4. As part of Qwest's training program, sales personnel are instructed to obtain supervisory approval of any proposed outbound marketing request. Business units within Qwest maintain a record of their sales and marketing campaigns that use CPNI. Those records include a description of each campaign, the specific CPNI that was used in the campaign, the date and purpose of the campaign, and the products or services offered. The records are maintained for a minimum of one year.

5. In those cases where Qwest agents or vendors have access to CPNI, Qwest also trains its agents and vendors that market Qwest products and services on the CPNI rules. Qwest's contracts contain a variety of protections regarding CPNI, including provisions limiting the use of CPNI to those purposes for which it is provided and prohibiting the improper disclosure of CPNI.

6. Qwest maintains a Quality Assurance group which observes and records customer calls. That Group monitors calls for, among other things, compliance with the CPNI rules and correct customer authentication. It provides feedback to managers for training purposes and if appropriate, disciplinary action.

7. Qwest has also established and documented disciplinary procedures for the enforcement of its CPNI standards outside of the Quality Assurance process. A potential violation of CPNI rules is investigated, and, where appropriate, disciplinary action is taken. In addition, Qwest maintains an advice line that employees may use to report violations of Company policies and practices, including improper use of CPNI.

8. Qwest takes reasonable measures to discover and protect against attempts to gain authorized access to CPNI. Qwest performs routine security evaluations and security assessments on Qwest systems, including those containing CPNI. Additionally, the Information Security and Technology group performs external penetration tests on Internet-facing web portals to ensure proper security is maintained. These activities further ensure that the necessary information-security safeguards are maintained with respect to CPNI and other customer information.

9. In addition to the general oversight activities described above, in response to the FCC's *2007 CPNI Order,* Qwest took the following actions:

    a) Qwest trained employees whose job responsibilities involve discussing account information over the telephone not to disclose call detail records absent special customer verification (*i.e.*, a password) unless the customer provides specific details about the call in question to the employee and the employee is responding to the information given by the customer.

b) Qwest modified its online access systems so that customer authentication now occurs without the use of biographical or account information. Customers affected by the rules (*i.e.*, customers that do not qualify for the "business exemption") must authenticate themselves using a Qwest issued security code to establish an online username and password for online-account access. Additionally Qwest established procedures to notify customers when passwords, a response to a back-up means of authentication for a lost or forgotten password, online account, or address of record are created or changed.

c) Qwest trained in-store employees to not release CPNI to customers unless they present a valid photo ID.

d) Qwest established procedures to notify law enforcement of an unauthorized disclosure of CPNI. Qwest informed all of its employees that they are required to report any unauthorized disclosure of CPNI to a central point for further investigation.